Indonesian Journal of Electrical Engineering and Computer Science
Vol. 42, No. 2, May 2026, pp. 469~484
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v42.i2.pp469-484

Enhancing IPv6 enabled IoT system security using addressless architecture

Ashmita Tiwari, Chitran Pokhrel, Babu R. Dawadi
Department of Electronics and Computer Engineering, Pulchowk Campus, Tribhuvan University, Lalitpur, Nepal

Article Info

Article history:

Received Oct 5, 2025
Revised Mar 4, 2026
Accepted May 26, 2026

Keywords:

6LoWPAN
Addressless architecture
Dynamic addressing
Elliptic curve cryptography
IoT security

ABSTRACT

The growth and sensitivity of internet of things (IoT) deployments demand robust and efficient security mechanisms, especially at the addressing layer. Traditional IPv6 addressing is susceptible to scanning, spoofing, and tracking, especially in IPv6 over low-power wireless personal area networks (6LoWPAN) networks. This paper proposes a dynamic elliptic curve cryptography (ECC)-based IPv6 address generation mechanism for 6LoWPAN IoT networks. Encrypting Interface IDs (IIDs) while keeping the network prefix the same to improve security against scanning, inference, and correlation attacks. High entropy of 0.9836 and cryptanalysis confirm higher randomness and high resistance to wide vectors of attacks. Having computed an average delay of encryption as 2.5728 ms, the process ensures low latency and insignificant overhead. It is more secure and efficient than existing techniques and hence is ideal for real-time resource- constrained IoT applications.

Corresponding Author:

Babu R. Dawadi
Department of Electronics and Computer Engineering, Pulchowk Campus, Tribhuvan University
Pulchowk, 44600 Lalitpur, Nepal
Email: baburd@ioe.edu.np

1. INTRODUCTION

Exponential growth of Internet of things (IoT) is revolutionizing industries by inter-connecting the network of billions of devices across the globe, leading to enhanced productivity, efficiency, and operational insight in industry automation, smart home, health care, and transport [1]. Despite its ability to transform, application of IoT technologies is hindered by fundamental security and scalability concerns, with one major vulnerability in current IoT implementations being the use of static IP addresses for device identification, which exposes devices to various threats [2]. Cyber-criminals exploit this by scanning known IP blocks to perform unauthorized intrusions, data extrusion, and distributed denial of service (DDoS) attacks [3]. This indicates the importance of advanced, context-aware, and scalable security designs that are purpose-built for IoT implementations.

Conventional IT security architectures, often designed for IPv4 networks, provide a minimum level of protection, they are insufficient when applied to the highly distributed, resource-constrained, and dynamic nature of IoT infrastructures [4]. Moreover, IPv4's major weaknesses—most notably, address space exhaustion [5]—make it ill-equipped to deal with the explosive growth in the number of IoT devices. To address the joint concerns of address-based targeting and static identity exposure, this paper introduces a novel IPv6 addressless framework for IoT networks using elliptic curve cryptography (ECC) to generate dynamic interface identifiers (IIDs) and leave the network prefix (NP) constant. This preserves the addressability and routing requirements of IPv6 but conceals device identity in the long term and thus neutralizes attacks based on predictable IP-based targeting. The novelty of the study is that, unlike existing

methods that rely on fixed or pseudo-random IID generation [6], the approach employs cryptographic entropy to ensure that every IID will be unpredictable and verifiable. In addition, this is among the first works incorporating ECC-based IID regeneration with a constant NP scheme to enable secure communication without disrupting network topology or causing additional
overhead. The major contributions the study presents are as follows:

- A novel IPv6 addressless architecture using ECC for secure, dynamic IID generation to protect device identity without altering the NP.
- A comprehensive analysis of the system's resilience against cryptanalytic, statistical, and spoofing-based attacks common in IPv6-enabled IoT environments.
- A performance validation using NS-3 simulation demonstrating low latency, jitter, and overhead along with a comparative analysis against exiting work in addressles architecture.

The rest of the paper is organized as follows: section 2 reviews relevant background and related work. In section 3 details the proposed method for dynamic address generation within the addressless framework. In section 4 discusses the experimental results and security evaluation. Section 5 is discussion and section 6 is conclusion. Finally, section 7 concludes the paper outlining limitations and potential directions for future research.

2. BACKGROUND AND THE RELATED WORK

The rapid expansion of IoT is, however, accompanied by historic security breaches following the finite computing capabilities, minimal memory, and power constraints of IoT devices. These constraints render it impossible or prohibitively costly to deploy conventional, resource-intensive security solutions such as those employed in standard IT infrastructures for the overwhelming majority of IoT applications.

IPv6 designed to address the scalability constraints of IPv4—essentially through its vast expanded address space—it also introduces complexities. Stateless address auto-configuration (SLAAC) and DHCPv6 features allow devices to auto-configure themselves, thereby allowing for quicker deployment and reduced administrative burden [7]. But these features also inadvertently expose IoT devices to address-based attacks since the generation process of the address is adhering to predictable behavior which can be used by attackers as reconnaissance or successful breach [8]. Moreover, all such practices like EUI-64-based IID generation, including the MAC address in the IPv6 address, only serve to further erode privacy by making hardware-level identifiers available and enabling device tracking over networks [9], [10].

To mitigate such threats, different alternative addressing and security solutions have been proposed by researchers. For instance, the 6LowPSec protocol [11] integrates lightweight link-layer security specifically for low-power IoT networks but fails to completely avoid address traceability. Other solutions such as crypto- graphic IIDs and dynamic address randomization [12] try to conceal device identities through uninterrupted IP address changes, hence making permanent tracking and attack targeting more difficult. One promising direction here is the use of addressless designs that reduce or even conceal accountable addressing information to make third-party mapping or probing of the network topology challenging [13], [14]. Such architectures typically come with encryption-based dynamic addressing, where cryptographic methods are used to generate fleeting or session-based IIDs that are difficult to statically analyze and predict. Among cryptographic methods deployable in such settings, ECC stands out due to its ability to pro- vide reasonable security guarantees employing smaller keys and minimal computational expense [15]. ECC is therefore particularly well-suited for resource-constrained IoT devices where conventional public-key techniques like RSA are too processor-intensive in terms of processing power, memory consumption, and power consumption [16]. Therefore, ECC-based systems have emerged as the ideal solution for encrypting next-generation IoT networks, especially with IPv6. With the growing use of IPv6 in the IoT networks, some re-searchers have proposed light-weight address-aware security protocols that can be used in resource-constrained environments. They aim to strike a balance between the need for secure security and IoT devices' low processing, memory, and power resources.

Sharma and Dhiman [17] have introduced SLAPSH, a light-weight and secure authentication protocol exclusively for smart home IoT devices. Sharma and Dhiman's scheme for reducing computational overhead along with protection against impersonation and replay attacks—two very common attacks on IoT systems. NS-3 simulation verification and AVISPA tool verification supported the feasibility and security efficacy of SLAPSH, thereby making it a great candidate for consumer-level IoT systems.

Perumal [18] explored threats in IoT networks with 6LoWPAN, the de facto standard for low-power wireless communication. The work, which was founded on Contiki OS and the 6LoWPAN protocol stack, underscored the need for inherent, built-in security in extremely resource-constrained devices, with the caveat that security in such systems cannot be an afterthought. In consideration to large-scale deployments, Wang *et al.* [19] presented a self-organizing massive IoT (MIoT) system with IPv6-based communication,

resource allocation, and routing optimization support. Their work demonstrated how clever architectural design was able to come at the expense of energy efficiency and scalability without disrupting interoperability within the network.

Sherburne *et al.* [20] mitigated the reconnaissance and DoS attacks by moving target defense (MTD) methods through randomization of IPv6 addresses. The method was implemented to modify device addresses dynamically in order to limit their predictability, hence preventing attackers from tracing or identifying devices over time. Although efficient in disrupting reconnaissance, the method was tedious in issuing consistent addresses and routing stability.

Adeniyi *et al*. [16] discussed the applicability of ECC in power-restricted IoT devices. Although their study presented the feasibility of using ECC in such applications, it also discovered vulnerabilities such as man-in-the-middle attacks and suggested that even cryptography would have to be supplemented with dynamic identity protection in order to become completely secure.

Savolainen [21] examined scalable methods of IPv6 address configuration for dynamic and mobile IoT networks. While the research addressed the issue of mobility and network reconfiguration, it lacked privacy- preserving capabilities for devices that roam across various network locations or those operating in multi-hop topologies.

Verma *et al.* [22] focused on the deployment of IPv6-enabled IPsec in wireless sensor networks (WSNs) for enhancing communication confidentiality and integrity. Their findings, however, demonstrated performance bottlenecks due to the computational overhead of IPsec, which challenged the viability of comparable solutions in extremely resource-constrained IoT settings.

Despite the profound contributions of these efforts, an end-to-end solution that covers lightweight encryption, dynamic IPv6 address management, and strong privacy assurances remains lacking. The majority of the proposed methods lack adaptive security controls or introduce overhead and complexity out of tune with real-world IoT deployments. Particularly, methods lack adequately in handling dynamic identity hiding, pre-predictable IID generation, and cross-compatibility with the heterogeneous IoT devices. That emphasizes a critical need for an economically viable, IPv6-supporting, and cryptographically sound architecture that delivers secure communication, device anonymity, and network robustness without compromising performance or scalability.

3. METHOD

The basic intention of this study is to offer solutions to significant concerns of privacy and security as- sociated with traditional static addressing methods in IoT communications and to support flexible and efficient management of addresses for IoT deployment scenarios. To emulate and validate the targeted system, NS-3 simulation was conducted since it is among the popular discrete-event network simulators whose capability to model realistic IoT environments accurately is of the highest quality [23]. This hybrid mesh topology had 30 IoT nodes. The choice of 30 nodes was deliberate, as it represents a typical and diverse communication environment in a mid-scale industry or enterprise. This setup is sufficient to study basic performance metrics like latency, traffic rate, and security activity, reflecting realistic scenarios such as intelligent building networks or local smart grid installations [24].

The hybrid-mesh topology was selected because it integrates device-to-device (D2D) and device-to-server communication, reflecting actual IoT environments where local interactions exist alongside centralized data gathering [25], [26]. Under this setup, nodes communicate with nearby devices and periodically report to a central server. The hybrid mesh topology model enhances the realism of the simulation and enables both routing efficiency and address verification schemes to be tested under various load and security settings [27]. The complete process of ECC-based address generation, including the interaction between nodes and the server, is illustrated in Figure 1.

In the proposed address allocation scheme, each IoT node generates a unique IPv6 IID using ECC-based cryptographic operations. During initialization, every device independently generates an ECC key pair consisting of a private key and a public key. The public key is computed as P=kG, where k is the randomly selected private key and Gis the base point on the elliptic curve defined over a finite field Fp. From this public key, the x-coordinate Px is extracted and passed through the SHA-256 cryptographic hash function. The final 64 bits of the hash output are used as the node's IID. This value, when appended to an IPv6 NP, forms the device's full IPv6 address.

This encryption mechanism makes the IID secure and distinct for each node, which prevents spoofing or duplication to a very large extent. To maintain long-term privacy and prevent tracking for a long time, each node also periodically refreshes its IID by generating a new ECC key pair. The refresh process creates a new hash output and thus a new IID without the need for central coordination.

On the server side, there is a validation system that ensures that only genuine IoT devices can join the network. During a received connection request, the server decrypts the public key part of the received IPv6 address using the stored private key. Its next re-computes the hash and compares with the received IID for validation. If the response is consistent, the device is authenticated, and communication is permitted. This step of cryptographic authentication gives good security without the overhead of maintaining large address registries. To formally describe the address generation process, the steps involved in generating the ECC-based IPv6 IID are summarized in Algorithm 1.

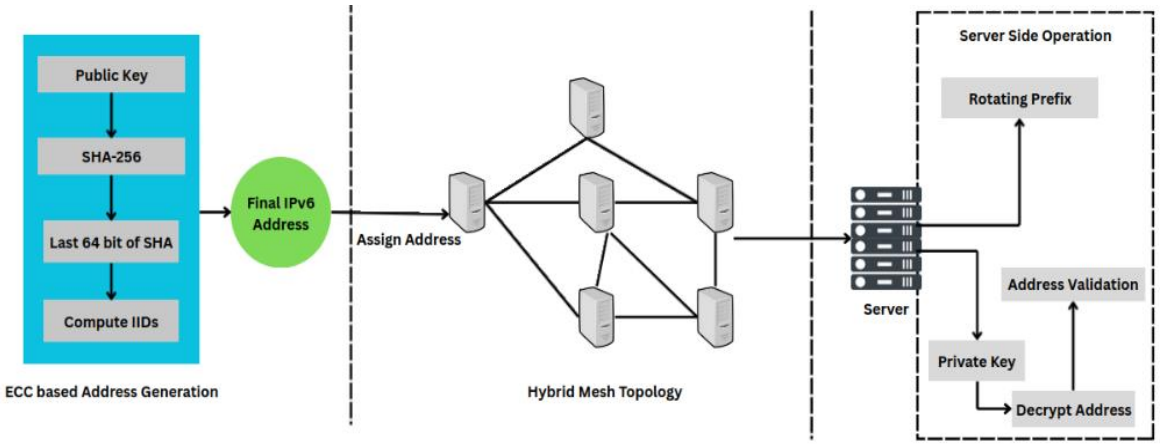

Figure 1. Illustration of ECC-based dynamic IPv6 address generation for 6LoWPAN enabled IoT device in hybrid mesh topology along with operations that occur in each side

Algorithm 1. ECC-based dynamic IPv6 interface identifier (IID) generation

Require:
Private Key k: A randomly generated secret key
Public Key P: Computed from k using the elliptic curve
Curve Parameters (a, b): Parameters defining the elliptic curve y2 = x3 + ax + b over a finite field Fp
Hash Function H: A cryptographic hash function
Ensure:
Interface Identifier (IID) AIID: A dynamically generated 64-bit IID for IPv6
procedure GENERATEINTERFACEID
Step 1: ECC Key Pair Generation
Select elliptic curve E over finite field Fp
Generate private key k∈Fp randomly
Compute public key P = (Px, Py) = kG, where G is the base point
Step 2: Compute IID
Extract the x-coordinate Px of the public key P
Compute hash H(Px) = SHA-256(Px)
Let AIID = Last 64 bits of H(Px)
Step 3: Periodic IID Renewal
To renew the IID, update k with a new random value
Recompute P = kG and regenerate the IID using Steps 2-3 18:
end procedure

4. RESULTS AND ANALYSIS

To evaluate the effectiveness of the proposed addressless IPv6 architecture, several performance and security metrics were analyzed. The experiments were conducted using the NS-3 simulator, with 30 nodes configured in a 6LoWPAN-enabled hybrid mesh topology. Metrics such as latency, throughput, jitter, entropy, and resistance to various forms of cryptanalysis were systematically measured to determine the reliability and robustness of the proposed system. Simulation protocols and parameters used for the experimentation purpose are listed in Table 1.

Table 1. Simulation parameters, protocols and tools used for IoT 6LoWPAN networks

Parameter	Value
Simulation tool	NS-3
Number of nodes	30
Network topology	Hybrid mesh
Link type	Point-to-point
Link data rate	100 kb/s
Link delay	10 ms
Network layer protocol	IPv6
IPv6 address base	fd00::/64
Dynamic IPv6 address generation	Time-based unique (ECC)
Transport layer protocol	UDP
Application type	OnOff
OnOff data rate	100 kb/s
Packet sink port	9
Simulation start time	0 seconds
Packet sink start time	1 second
Packet sink stop time	10 seconds
OnOff start time	2 seconds
OnOff stop time	10 seconds
6LoWPAN	Enabled

4.1. Evaluation of security parameters

The evaluation of security parameters—including entropy analysis, pattern detection, and cryptanalytic testing—demonstrates the robustness of the ECC-based dynamic address generation scheme. While the entropy determines the randomness in generated IIDs and its representation. The cryptanalysis highlights on level of resistance to a wide range of attacks, including statistical inference, differential and linear approximations, and brute-force attempts, obtained by minimizing structural redundancy [28]. The following subsections present a detailed analysis and interpretation of each evaluation method.

4.1.1. Analysis of entropy

The Shannon entropy of 30 different ECC generated addresses was computed in this test. Observe that the NP of these nodes remained unchanged but the IID changed. This study is intended measure the degree of randomness and unpredictability of the ECC generated address by computing the entropy of all cryptographic addresses which are visible to intruders. The actual IPv6 address is only shown to the internal system. Cryptographers can utilize this information to examine how well the encryption scheme conceals the original content (in this case actual address) [29]. Greater entropy is more secure as it contains a greater amount of randomness, and therefore it is almost difficult to decrypt by any unauthorized parties. The calculated entropy for ECC generated address for 30 different nodes are shown in Figure 2 and the statistics for the entropy values are shown in Table 2.

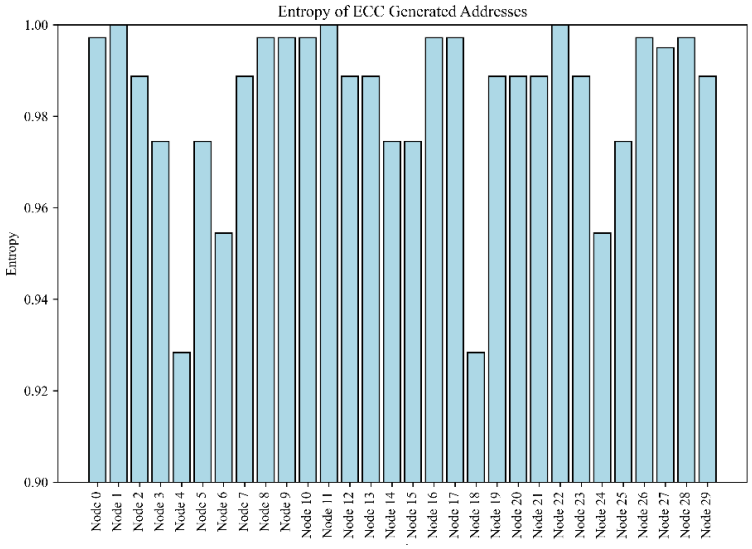

Figure 2. Entropy of ECC generated addresses (cryptographic address) for 30 different nodes visible to the intruders trying to target the network

Table 2. Entropy statistics for ECC-generated dynamic IPv6 address

Statistic	Value
Count	30
Mean	0.9836
Standard deviation	0.0194
Minimum	0.9284
25% percentile	0.9745
50% Percentile (median)	0.9887
75% percentile	0.9972
Maximum	1.0000

The entropy values in Table 2 confirm a high level of randomness and unpredictability in the dynamic IPv6 addresses produced by ECC. With an average entropy value of 0.9836, the distribution of byte values in the produced addresses is nearly uniform, with very little room for pattern recognition or predictability. The standard deviation of 0.0194 also bears testament to this fact, with entropy values clustered around the mean with less fluctuation. Breakdown of 25th, 50th, and 75th percentiles—0.9745, 0.9887, and 0.9972 respectively—demonstrates that strong entropy is maintained in all segments of data with the median being close to 1.0, confirming that most addresses present strong randomness in a uniform way. The extremes, 0.9284 and 1.0000 respectively, validate the observation: the least random address still has a high entropy rating, and the most random approaches optimal unpredictability. The overall entropy profile here shows that the ECC- based address-generation method effectively ensures security through randomness and significantly reduces the possibility of pattern-detection and statistical inference-based attacks [29], [30].

From a security perspective, the persistently high entropy of ECC-generated dynamic IPv6 addresses evidences strong resilience against attacks based on exploitable predictability patterns, such as brute-force or structural inference attacks [31]. The high level of randomness ensures confidentiality and prevents unauthorized entry or reverse-engineering of address structures.

4.1.2. Differential cryptanalysis for ECC generated IPv6 addresses

Differential cryptanalysis relies on the impact differences between actual inputs have on differences in cryptographic output in an attempt to identify the strength and security of the cryptographic algorithms [32]. In attempting to reveal the secret key or the inner cipher process, the technique looks for correlations or patterns that exist during the encryption process. For differential analysis the byte difference value in actual address were matched with the difference value in ECC generated IPv6 as shown in Figure 3.

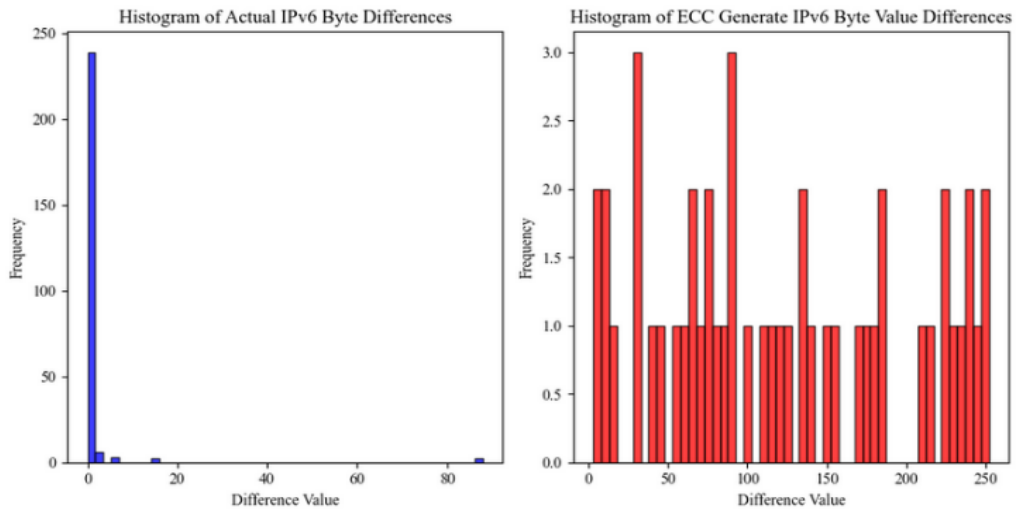

Figure 3. Histogram of byte difference value for actual IPv6 (left) and ECC generated IPv6 (right). The actual address represents the address visible to the internal network components.

Figure 3 histograms represent actual IPv6 addresses vs. ECC-based generated addresses' byte-level difference patterns. The left histogram of actual IPv6 addresses presents a non-uniform distribution with differences clustered around zero, with minimal variations among consecutive addresses and patterns'

predictability. The right histogram of ECC-generated addresses illustrates a uniform distribution, indicating high randomness and lack of correlation between difference addresses. From a differential cryptanalysis point of view, this uniformity ensures that ECC-based address generation effectively shatters detectable patterns, making it much harder for attackers to carry out inference or correlation-based attacks. The unpredictability introduced by ECC thus introduces privacy and security by minimizing risks such as address scanning and tracking.

For security reasons, this implies that dynamically assigned ECC-based IPv6 addresses have improved resistance to differential or statistical cryptanalytic attacks. Uniform distribution of differences avoids predictability of future addresses from observations in history [33] due to which it reduces the threat of prefix hijacking, replay attacks, and IPv6-based reconnaissance attacks. Randomness renders it more private since it is harder for the attackers to track the users using their dynamically assigned IPv6 addresses. However, further cryptographic analysis must be performed to ensure the absence of potential vulnerabilities, such as hidden structural bias in the ECC-based generation process.

4.1.3. Linear cryptanalysis for ECC generated IPv6 addresses

Linear cryptanalysis plays an important role in the study of the strength of encryption algorithms as it presents a systematic approach to uncovering design weaknesses in the cipher by establishing the linear approximations that best describe its operation [32]. Linear cryptanalysis illustrates how well an algorithm applies the confusion and diffusion properties sought after by the assurance that the relationship between plaintext, cipher-text, and key is complex and non-linear [34]. Throughout this experiment, linear cryptanalysis was performed by analyzing bit correlation as shown in Figure 4.

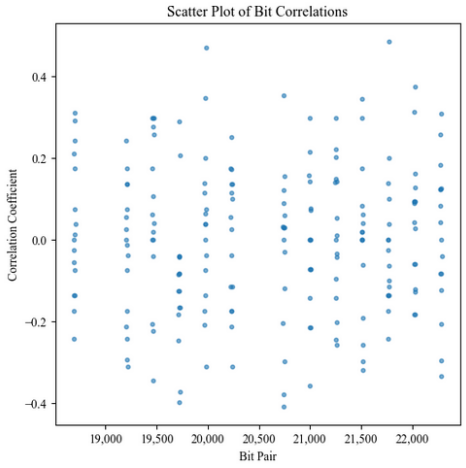

Figure 4. Scatter plot illustrating the correlations between bit pairs in ECC generated IPv6 addresses

Figure 4 is a scatter diagram of the correlation between different pairs of bits of an ECC-based dynamically generated IPv6 address. The scatter plot of correlation coefficients is random around zero with no clustering or recognizable patterns of high correlations. This confirms the lack of a strong linear relationship between pairs of bits, which is a necessary condition for withstanding linear cryptanalytic attacks. Where there exist high correlations between some pairs of bits in a cryptographic system, adversaries can utilize such predictable correlations to deduce secret keys or future values, breaking the system which is not the case here. The absence of linear relationship is more evident in the distribution plot of the correlation coefficients given in Figure 5.

The density plot in Figure 5 provides further statistical data on the correlation coefficients, with the note that they are nearly normally distributed with zero at the center. Symmetry and spread of the distribution suggest that there are no significant linear biases, which means any linear approximation of the bit relationships would be highly unreliable. In linear cryptanalysis, an attacker attempts to exploit statistical biases in the ciphertext and plaintext bit relationships. The lack of strong biases in this case suggest that an attacker who attempts to uncover linear approximations would struggle to gain a significant advantage in predicting address transformations.

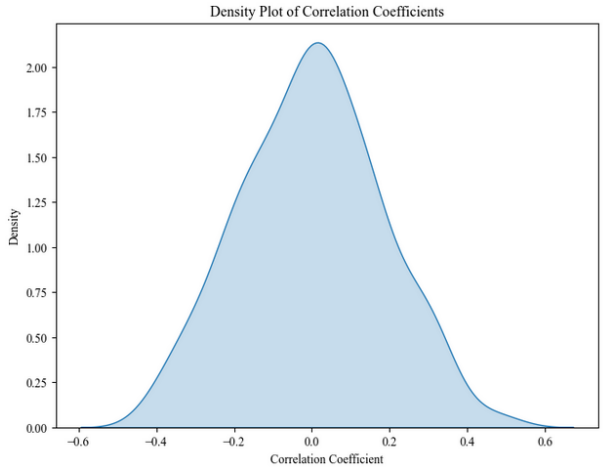

Figure 5. Density plot for correlation coefficients of Bit pairs for ECC generated IPv6 addresses

From a security perspective, such results imply that the ECC-based IPv6 address generation method is highly resistant to linear cryptanalysis. Since the bit relationships have no exploitable linear structure, it becomes computationally hard for an attacker to use linear approximations to break the scheme. This enhances the system's resistance against statistical dependence-based crypt attacks, thus making it a more secure option for dynamic IPv6 address generation. Other non-linear cryptographic techniques, however, must be explored for general security guarantee.

4.2. Evaluation of network parameters

Network parameter analysis was conducted by simulating a network in which packet delivery information was monitored and stored into PCAP files. The PCAP files preserve packet level detail of network data with packet times, source and destination IPs, protocol metadata, and packet payload. Upon simulation completion, multiple PCAP files were concatenated into a combined dataset appropriate for analysis.

The latency distribution graph in Figure 6 presents a right-skewed trend, where most of the latency values are clustered between the range 10–20 ms, with a tall spike at 10–15 ms, referring to the best-case performance under normal circumstances. However, occasional high-latency outliers of as much as 49.71 ms suggest occasional delays, perhaps due to the computational overhead of ECC operations, network congestion, or resource limitations of IoT devices [35]. Such latency spikes are undesirable for time-sensitive applications like industrial automation or healthcare monitoring [36], where dependable low-latency communication is essential. The statistics for latency can be observed in Table 3.

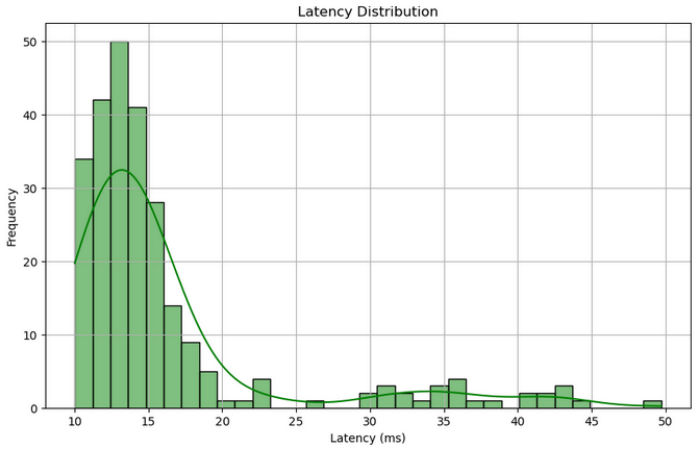

Figure 6. Latency distribution for simulation with 6LoWPAN enabled 30 nodes IoT device

As Table 3 describes, the average latency is 16.14 ms and standard deviation of 7.62 ms, indicating high variability in delay but low consistency. A minimum of 10.02 ms also confirms that the system can easily achieves low delay under ideal circumstances, whereas maximum being as high as 49.71 ms reveals the system not to be stable. Although the median and mean latency of 13.70 ms and 16.14 ms respectively, falls well within acceptable limits for industrial and real-time operations which require below 60 ms delay [37], occasional spikes may lead to undesirable issues such as lag or buffering. To enhance the reliability and performance of 6LoWPAN networks, especially under fluctuating network loads, optimizations like lightweight cryptography, efficient routing, and adaptive resource allocation are necessary.

Table 3. Latency statistics for 6LoWPAN enabled IoT network

Statistic	Value (ms)
Mean	16.143230
Standard deviation (std)	7.615924
Minimum (min)	10.021000
25th percentile (Q1)	12.055000
Median (Q2)	13.703500
75th percentile (Q3)	15.927000
Maximum (max)	49.709000

The distribution curve of throughput in Figure 7 appears bimodal, indicating two performance states of the 6LoWPAN-capable IoT device. The earlier peak in the range of 30,000–40,000 Bps represents poor operational states predominantly caused by network congestion, interference, or overheads of ECC-based IPv6 address computation. The larger peak observed in the range of 80,000–100,000 Bps represents mean throughput under optimal network operation. A good-fitting curve shows a left-skewed trend, i.e., high throughput is typical with bursts of dips in the mode of processing or network volatility. To mitigate such bursts, enhancements such as lightweight cryptographic algorithms, energy-efficient routing protocol, and adaptive resource handling must be done [38].

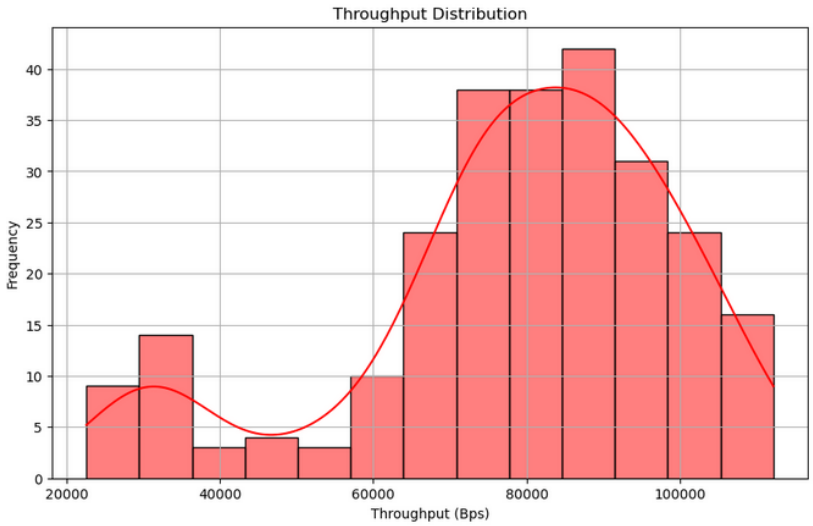

Figure 7. Throughput distribution for 6LoWPAN enabled 30 node IoT devices

Observation from Table 4 suggests that the average throughput is 78,690.90 Bps and standard deviation is 20,923.49 Bps with medium data rate variability. There is a difference of minimum 22,611.51 Bps to maximum 112,163.39 Bps reflecting the performance of the system under stressed and peak loads. The 75th and 25th percentiles (93,237.80 Bps and 70,573.54 Bps, respectively) and the median throughput of 82,021.79 Bps also indicate this dual-behavior characteristic. This two-mode distribution further indicates that the device switches between two work modes—one showing full functionality and another showing resource- or network-evoked limitations—bearing implications on overall network reliability and responsiveness in IoT applications.

Table 4. Statistical summary of throughput (Bps) for 6LoWPAN enabled IoT network

Statistic	Throughput (Bps)
Mean	78,690.90
Standard deviation (std)	20,923.49
Minimum (min)	22,611.51
25% quartile (Q1)	70,573.54
Median (50%)	82,021.79
75% quartile (Q3)	93,237.80
Maximum (max)	112,163.39

The graph of Jitter distribution as shown in Figure 8 for the 6LoWPAN IoT device shows a distribution that is skewed towards the right, whereby the majority of the jitter values are found to be in the 0-5 ms range but have some scattered points beyond 30 ms. The large concentration of low jitter values guarantees that the network has a stable transmission rate with minimal packet delay variation. However, the long tail of the distribution suggests that these spikes of jitter do exist and can be a result of random fluctuations in strength of connectivity, delay in crypto math, or congestion in a network. For real-time critical use such as video conferencing or VoIP, and IoT the tolerable jitter value is below 30 ms [39] so outliers make time-base applications that utilize guaranteed packet-delivery intervals such as VoIP, real-time monitoring, and industrial control networks unstable.

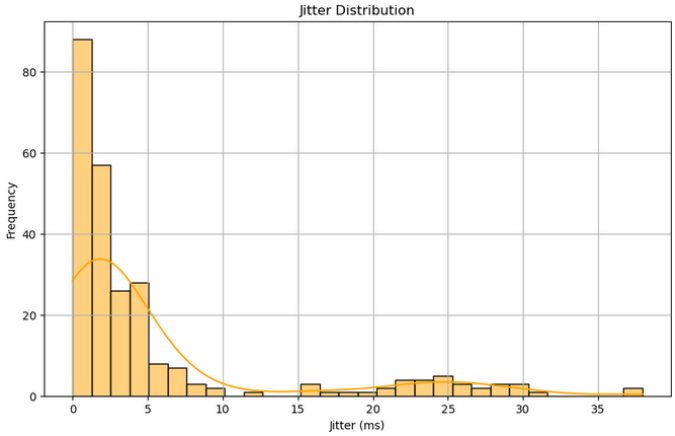

Figure 8. Jitter distribution for 6LoWPAN enabled IoT nodes in hybrid mesh topology

Table 5 show certain delay variability, with a mean jitter of 5.39 ms and a high standard deviation of 8.16, while values range from a minimum of 0.009 ms to a maximum of 37.94 ms—indicating occasional extreme fluctuations. Although jitter is low in most situations, these extremes reflect periodic network instability, packet reordering, delay buffering, and impaired QoS, particularly in time-sensitive applications [40]. To correct this, the buffering, jitter compensation, and higher-level routing need to be in place to allow effective and fault-free communication in high-stakes IoT systems [41].

Table 5. Jitter Statistics

Statistic	Value (ms)
Mean	5.392216
Standard deviation (std)	8.162640
Minimum (min)	0.009000
25th Percentile (Q1)	0.905000
Median (Q2)	2.110000
75th Percentile (Q3)	4.661000
Maximum (max)	37.944000

Figure 9 illustrates a negative relationship between throughput and latency in an ECC-supported 6LoWPAN-based IoT system for dynamically assigning IPv6 addresses. Initially, when latency is minimal (in the range of 10–20 ms), throughput is at its maximum, over 100,000 bps. With increasing latency,

throughput drops rapidly, exhibiting an exponential decline trend. From 25 ms and above, the drop in throughput becomes linear, indicating a point of saturation beyond which further latency has a marginal impact. This trend reflects the latency sensitivity of low-power IoT networks that intrudes upon data transmission effectiveness.

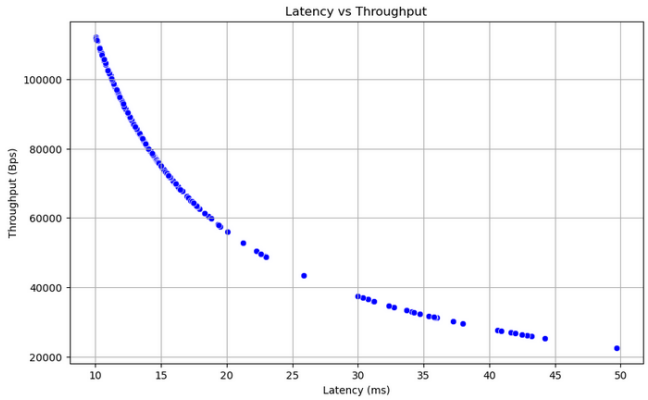

Figure 9. Evaluating performance of throughput as the latency increases

The results show that while ECC-based IPv6 address generation may provide security, it introduces computational complexity that introduces latency and reduces throughput. The expense is high in resource-limited IoT networks where security can be optimized with minimal impact on performance. Network designers must balance cryptography computation, transmission delay, and bandwidth usage to enable secure communication in 6LoWPAN networks at reasonable latency and throughput rates.

4.3. Comparative analysis of proposed ECC based dynamic address generations for addressless architecture against existing work in addressless architecture

To evaluate the effectiveness of the proposed addressless architecture, it is essential to compare its performance with existing approaches in the same domain. Most prior works have primarily focused either on service module-based designs or on dynamic address fusion techniques [14]. A notable and closely related study by Liu *et al.* [42] regarding IoT server security employs ECC along with other algorithms to dynamically generate IPv6 addresses, including NP. Their work has been validated in a large-scale hybrid mesh topology involving over 1,000 nodes, making it a relevant benchmark for comparison. However, the test of our proposed mechanism was not possible for 1,000 nodes due to available computational resource constraints with devices for simulation. Therefore, a 30-node test scenario was conducted with architecture as shown in Figure 10 and with similar method used in Liu's work [42] simulated in NS-3. The comparative results are shown in Table 6.

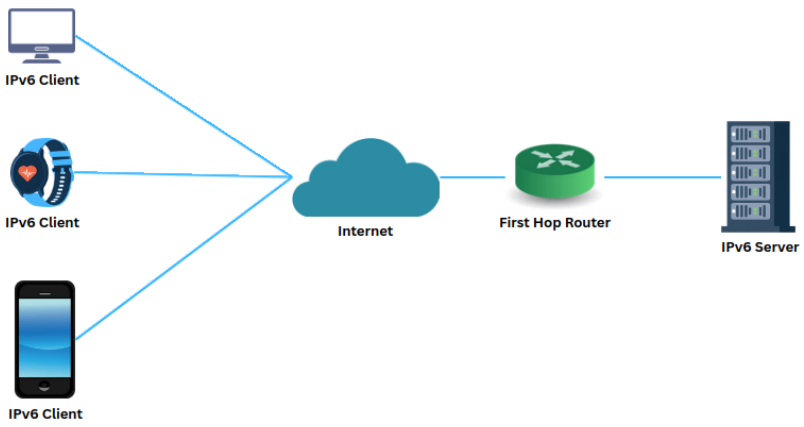

Figure 10. Topology of addressless IoT server used in the exiting work on addressless architecture [42]

Table 6. Comparative study: proposed method vs. Liu's work with 30 nodes configuration

Criteria	Proposed method (in Ns-3)	Liu's method (in NS-3)
Nodes	30	30
Dynamic address generation	ECC (IID)	ECC (NP + IID)
Topology	Hybrid mesh	Hybrid mesh
Address entropy	0.9836	0.9733
Average latency	16.143230 ms	20.235631 ms
Average jitter	5.392216 ms	6.424116 ms
Average address encryption/generation delay	2.5728 ms	4.5 ms
Average address verification/validation delay	2.5768 ms	6.4 ms

Table 6 presents the comparison analysis of the proposed method and the Liu *et al.* [42] scheme, both implemented with a 30-node hybrid mesh topology and elliptic curve cryptography (ECC) being utilized for dynamic address generation. While both methods preserve the security benefits of ECC, the proposed method achieves a slightly higher address entropy of 0.9836, compared to 0.9733 in the case of Liu *et al.* [42] scheme. This increase resonates with a more uniform distribution of address space that works to enhance anonymity, reduce exposure to address correlation attacks, and offer improved resistance to identity tracking—a critical element in privacy-centric IoT environments.

Regarding communication efficiency, the proposed method put forward is more efficient than the baseline in terms of latency and jitter. The latency was reduced from 20.24 ms to 16.14 ms, a reduction of 20.2%. Similarly, the jitter went down from 6.42 ms to 5.39 ms, which is improved temporal stability of packet transmission. These enhancements are attributed to efficient address dissemination mechanisms and efficient packet forwarding methods in the hybrid mesh structure, which shows that the proposed system is better suited for real-time and delay-sensitive IoT applications.

The new method also performs better in cryptographic operations with respect to address handling. The average address encryption or generation delay reduces to 2.5728 ms from Liu *et al.'s* [42] 4.5 ms, and the address verification or validation delay reduces from 6.4 ms to 2.5768 ms. These reductions indicate a more efficient ECC implementation of operations, possibly due to lightweight cryptographic optimizations. Because address management is such a frequent operation in privacy-aware and dynamic IoT networks, eliminating such delays becomes central to overall system scalability and responsiveness [43].

4.4. Comparative study of ECC based dynamic address generation against static address generation

To evaluate the performance differences between ECC-based address generation and traditional static address architectures, an NS-3 simulation was conducted using identical network topologies and the same number of nodes, each configured with 6LoWPAN-enabled static IPv6 addresses. Packet captures from the simulation were then analyzed to measure key network parameters. The observation between static and ECC based dynamic address generation is as shown in Table 7.

The comparative analysis in Table 7 highlights that ECC-based dynamic address generation provides much greater security than traditional static addressing by way of much greater entropy value (0.9836 vs. 0.558831). The greater entropy guarantees greater randomness, and addresses become harder to guess or track and hence impart strong immunity against spoofing, reconnaissance, and tracking attacks [30].

Static addressing, however, generate predictable patterns which expose the network to numerous attacks and therefore is not appropriate for high-priority IoT scenarios. Security improvements with ECC, however, comes with some performance cost. The ECC-based scheme involves higher average latency (16.14 ms compared to 11.90 ms), slightly higher jitter (5.39 ms compared to 5.35 ms), and lower average throughput (78,690 Bps compared to 116,832.91 Bps) because of added computational overhead by cryptography. Though this degrades performance, in application scenarios where security comes at any price—critical infrastructure and privacy-sensitive IoT applications—the compromise is tolerable. The ECC-based approach offers a safer foundation for communications, but with some sacrifice to raw performance levels.

Table 7. Comparative study: ECC-based proposed method vs. static address method

Criteria	ECC-based proposed method	Static address generation
Nodes	30	30
Dynamic address generation	ECC	-
Topology	Hybrid Mesh	Hybrid Mesh
Address entropy	0.9836	0.558831
Average latency	16.143230 ms	11.896 ms
Average jitter	5.392216 ms	5.354 ms
Average throughput	78,690 Bps	116,832.913 Bps

5. DISCUSSION

The study evaluated a lightweight and secure IPv6 addressless architecture for 6LoWPAN-enabled IoT system. The findings reveal that the ECC-based dynamic generation of IPv6 addresses significantly enhances 6LoWPAN-capable IoT network security. By dynamically generating the IIDs while keeping the NP constant, the scheme effectively prevents tracking, spoofing, and scanning attacks that are common with static identity exposure and address-based targeting. The simulation results confirmed high address entropy (average 0.9836) indicating resistance against interference and scanning attacks by thwarting address format or node location identification with random byte distribution. The study also show strong resistance to cryptanalysis, and low encryption delay (2.5728 ms), all while maintaining acceptable latency, jitter, and throughput. Furthermore, cryptographic binding of private keys to addresses prevents from spoofing attacks and DDoS attacks are precluded by dynamically changing cryptographically secured addresses, which reduce traffic flooding activities to a bare minimum. The linear and differential cryptanalysis further proves that there is also statistical independence of the addresses generated, so it is difficult for attackers to use mathematical approximations to reverse-engineer addresses.

While most of the prior works primarily focused either on service module-based designs [13] or on dynamic address fusion techniques [14], they fall short when compared to addressless architecture-based approach. This is due to the fact that both module-based designs and dynamic address fusion techniques rely on predictable or semi-static identifiers, making them more vulnerable to tracking, spoofing, and scalability issues. Compared to prior work on addressless architecture [42] that utilized cryptographic application for dynamic IPv6 address generation that modifies both NP and IID, the proposed approach achieves improved entropy and lower delay, offering a more efficient solution for real-time, resource-constrained environments.

6. CONCLUSION

In conclusion, the ECC-based address generation scheme offered greater IoT network security by preventing attacks on address predictability and weak cryptographic infrastructure. The high entropy, non-linear transformations, and statistical independence offer resistance against spoofing, scanning, DDoS, tracking, and cryptanalysis. The system operates efficiently with low latency and jitter, and therefore it is well suited for resource-constrained environments. Overall, the findings are relevant to IoT researchers and engineers as they address static IP vulnerabilities using a lightweight ECC-based dynamic addressing scheme. This solution not only secures IoT networks but also offers a scalable and efficient approach to real-time use cases, strengthening defenses against a broad spectrum of attack vectors.

7. LIMITATIONS AND FUTURE WORK

While the suggested ECC-based dynamic IPv6 address generation model possesses robust security. and effective performance, there exist some limitations that have to be weighed in order to realize its usability in real-world applications. The limitations are:

- The simulation was conducted on a small-scale network of 30 nodes, which may not fully represent the behavior of larger, more complex IoT environments.
- The system assumes secure storage and distribution of ECC private keys, which in practice can be vulnerable, especially in low-resource devices.
- Power consumption and energy efficiency were not evaluated, even though these are critical factors in battery-operated or remote IoT nodes.
- Address regeneration intervals were static and not based on context-aware or adaptive mechanisms that respond to network or threat conditions.
- It was tested in a controlled simulation environment, which may not reflect the impact of unpredictable factors like node failures, packet loss, or network congestion.
- The study does not address the internal threats that may be possible in real-world deployment of IoT networks.

Future work: following the promising results and limitations of this study, the following directions are assessable for future research to enhance ECC-based dynamic IPv6 address generation framework. The future works are:

- Scaling simulations to large-scale IoT networks with hundreds or thousands of nodes to evaluate scalability, performance bottlenecks along with management overhead.
- Designing and integrating lightweight and secure ECC key distribution protocols for constrained IoT environments, such as ECC-based Diffie-Hellman or identity-based cryptographic schemes.
- Optimizing and analyzing power consumption of the ECC-based address generation to achieve energy efficiency for battery-powered devices.

- Incorporate adaptive and context-aware address regeneration techniques that adjust the frequency of address updates based on risk levels, traffic patterns, or environmental conditions.
- Mimic actual-world attack scenarios like key compromise, and traffic analysis to verify the robustness of the framework under active attack.
- Perform distributed key management for fault tolerance, and test the strength of the proposed method against the quantum algorithm-based attacks.

FUNDING INFORMATION

This research was partially supported by Nepal Academy of Science and Technology (NAST) under small research grants (grant (ID: NRG-080/81-Engg-01) principally investigated by Dr. Babu R. Dawadi.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ashmita Tiwari	✓	✓			✓		✓	✓	✓		✓			
Chitran Pokhrel	✓	✓	✓	✓	✓	✓			✓	✓	✓			
Babu R. Dawadi	✓	✓		✓	✓	✓	✓		✓	✓		✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors declare no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [initials:A.T. & C.P.], upon reasonable request.

REFERENCES

[1] S. Munirathinam, "Chapter Six - Industry 4.0: industrial internet of things (IIoT)," in *Advances in Computers*, vol. 117, no. 1, P. Raj and P. Evangeline, Eds., Elsevier, 2020, pp. 129–164. doi: 10.1016/bs.adcom.2019.10.010.
[2] V. Adat and B. B. Gupta, "Security in internet of things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems*, vol. 67, no. 3, pp. 423–441, Mar. 2018, doi: 10.1007/s11235-017-0345-9.
[3] R. Sabillon, V. Cavaller, J. Cano, and J. Serra-Ruiz, "Cybercriminals, cyberattacks and cybercrime," in *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, IEEE, Jun. 2016, pp. 1–9, doi: 10.1109/ICCCF.2016.7740434.
[4] D. Minoli, *Building the Internet of Things with IPv6 and MIPv6*. Wiley, 2013. doi: 10.1002/9781118647059.
[5] P. Richter, M. Allman, R. Bush, and V. Paxson, "A primer on IPv4 scarcity," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 2, pp. 21–31, Apr. 2015, doi: 10.1145/2766330.2766335.
[6] J. L. Shah and J. Parvez, "Optimizing security and address configuration in IPv6 SLAAC," *Procedia Computer Science*, vol. 54, pp. 177–185, 2015, doi: 10.1016/j.procs.2015.06.020.
[7] Y.-R. Li and G.-Y. Wei, "A research on IPv6 address auto-configuration for IoT," in *Proceedings of the 2nd International Conference on Telecommunications and Communication Engineering*, 2018, pp. 11–15.
[8] E. Tucker, "SLAAC vs. DHCPv6: choosing the right IP address assignment method." Accessed: May 23, 2026. [Online]. Available: https://netseccloud.com/slaac-vs-dhcpv6-choosing-the-right-ip-address-assignment-method.
[9] I. van Beijnum, *Running IPv6*. Berkeley, CA: Apress, 2006, doi: 10.1007/978-1-4302-0090-1.
[10] K. E. Thordarson, "Analysis of eui-64'based addressing and associated vulnerabilities," Naval Postgraduate School, California, 2020.
[11] G. Glissa and A. Meddeb, "6LowPSec: an end-to-end security protocol for 6LoWPAN," *Ad Hoc Networks*, vol. 82, pp. 100–112, Jan. 2019, doi: 10.1016/j.adhoc.2018.01.013.
[12] A. Venčkauskas, N. Morkevicius, V. Jukavičius, R. Damaševičius, J. Toldinas, and Š. Grigaliūnas, "An edge-fog secure self-authenticable data transfer protocol," *Sensors*, vol. 19, no. 16, p. 3612, Aug. 2019, doi: 10.3390/s19163612.

[13] S. Hao, R. Liu, Z. Weng, D. Chang, C. Bao, and X. Li, "Addressless: a new internet server model to prevent network scanning," *PLoS One*, vol. 16, no. 2, p. e0246293, Feb. 2021, doi: 10.1371/journal.pone.0246293.
[14] C. Liu, F. Chen, T. Wang, C. Zhao, D. Xie, and P. Hu, "A secure and dynamic fusion addressing scheme for internet of vehicles scenarios," *Computer Networks*, vol. 260, p. 111112, Apr. 2025, doi: 10.1016/j.comnet.2025.111112.
[15] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, no. 2, pp. 1515–1555, Feb. 2021, doi: 10.1007/s11276-020-02535-5.
[16] A. E. Adeniyi, R. G. Jimoh, and J. B. Awotunde, "A systematic review on elliptic curve cryptography algorithm for internet of things: categorization, application areas, and security," *Computers and Electrical Engineering*, vol. 118, p. 109330, Aug. 2024, doi: 10.1016/j.compeleceng.2024.109330.
[17] N. Sharma and P. Dhiman, "A secure addressing mutual authentication scheme for smart IoT home network," *Multimedia Tools and Applications*, vol. 84, no. 22, pp. 25111–25143, Aug. 2024, doi: 10.1007/s11042-024-19898-y.
[18] S. Perumal, "Escalation of security and privacy in internet of things using advanced IPv6 based security mechanism," *Wasit Journal of Computer and Mathematics Science*, pp. 33–39, Mar. 2021, doi: 10.31185/wjcm.Vol1.Iss1.7.
[19] G. Wang, J. Wang, A. Zhang, B. Liu, and C. Liu, "Design and application of 6LoWPAN-based metrology IoT for smart manufacturing enterprises," in *Proceedings of the 2023 5th International Conference on Internet of Things, Automation and Artificial Intelligence*, New York, NY, USA: ACM, Nov. 2023, pp. 90–95, doi: 10.1145/3653081.3653097.
[20] M. Sherburne, R. Marchany, and J. Tront, "Implementing moving target IPv6 defense to secure 6LoWPAN in the internet of things and smart grid," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14*, New York, New York, USA: ACM Press, 2014, pp. 37–40, doi: 10.1145/2602087.2602107.
[21] T. Savolainen, J. Soininen, and B. Silverajan, "IPv6 addressing strategies for IoT," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3511–3519, Oct. 2013, doi: 10.1109/JSEN.2013.2259691.
[22] S. Verma, Y. Kawamoto, and N. Kato, "A network-aware internet-wide scan for security maximization of IPv6-enabled WLAN IoT devices," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8411–8422, May 2021, doi: 10.1109/JIOT.2020.3045733.
[23] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "Computer network simulation with ns-3: a systematic literature review," *Electronics (Basel)*, vol. 9, no. 2, p. 272, Feb. 2020, doi: 10.3390/electronics9020272.
[24] M. Barton, R. Budjac, P. Tanuska, I. Sladek, and M. Nemeth, "Advancing small and medium-sized enterprise manufacturing: framework for IoT-based data collection in Industry 4.0 concept," *Electronics (Basel)*, vol. 13, no. 13, p. 2485, Jun. 2024, doi: 10.3390/electronics13132485.
[25] X. Jiang *et al.*, "Hybrid low-power wide-area mesh network for IoT applications," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 901–915, Jan. 2021, doi: 10.1109/JIOT.2020.3009228.
[26] M. Bano, A. Qayyum, R. N. Bin Rais, and S. S. A. Gilani, "Soft-mesh: a robust routing architecture for hybrid SDN and wireless mesh networks," *IEEE Access*, vol. 9, pp. 87715–87730, 2021, doi: 10.1109/ACCESS.2021.3089020.
[27] A. Kavitha *et al.*, "Security in IoT mesh networks based on trust similarity," *IEEE Access*, vol. 10, pp. 121712–121724, 2022, doi: 10.1109/ACCESS.2022.3220678.
[28] A. Sinkov, *Elementary Cryptanalysis*, vol. 22. Providence, Rhode Island: American Mathematical Society, 2009, doi: 10.5948/UPO9780883859377.
[29] W. Easttom, *Modern Cryptography*. Cham: Springer International Publishing, 2022, doi: 10.1007/978-3-031-12304-7.
[30] C. Swenson, *Modern cryptanalysis: techniques for advanced code breaking*. John Wiley & Sons, 2008.
[31] A. Okutan and S. J. Yang, "ASSERT: attack synthesis and separation with entropy redistribution towards predictive cyber defense," *Cybersecurity*, vol. 2, no. 1, p. 15, Dec. 2019, doi: 10.1186/s42400-019-0032-0.
[32] H. M. Heys, "A tutorial on linear and differential cryptanalysis," *Cryptologia*, vol. 26, no. 3, pp. 189–221, Jul. 2002, doi: 10.1080/0161-110291890885.
[33] X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," in *Advances in Cryptology — EUROCRYPT '91*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 17–38, doi: 10.1007/3-540-46416-6_2.
[34] J. Daemen, "Cipher and hash function design strategies based on linear and differential cryptanalysis," KU Leuven, Leuven, 1995. Accessed: Jun. 03, 2026. [Online]. Available: https://cs.ru.nl/~joan/papers/JDA Thesis 1995.pdf
[35] M. Iorio, F. Risso, and C. Casetti, "When latency matters," *ACM SIGCOMM Computer Communication Review*, vol. 51, no. 4, pp. 2–13, Oct. 2021, doi: 10.1145/3503954.3503956.
[36] S. Figueroa-Lorenzo, J. Añorga, and S. Arrizabalaga, "A survey of IIoT protocols: a measure of vulnerability risk analysis based on CVSS," *ACM Computing Surveys*, vol. 53, no. 2, pp. 1–53, Mar. 2021, doi: 10.1145/3381038.
[37] P. Ferrari, E. Sisinni, D. Brandao, and M. Rocha, "Evaluation of communication latency in industrial IoT applications," in *2017 IEEE International Workshop on Measurement and Networking (M&N)*, IEEE, Sep. 2017, pp. 1–6, doi: 10.1109/IWMN.2017.8078359.
[38] M. U. Mushtaq, J. Hong, M. Owais, and S. A. Danso, "Enhancing security and energy efficiency in wireless sensor network routing with IoT challenges: a thorough review," *LC international journal of stem (ISSN: 2708-7123)*, vol. 4, no. 3, pp. 1–24, 2023.
[39] T. Arbuthnot, "What are thresholds for good and poor network packet loss, jitter and round trip time for unified communications?," *Tom Talks, May*, vol. 17, p. 7, 2018.
[40] T. Eckert and S. Bryant, "Quality of service (QoS)," in *Future Networks, Services and Management*, Cham: Springer International Publishing, 2021, pp. 309–344, doi: 10.1007/978-3-030-81961-3_11.
[41] J. Cordero, J. Yi, and T. Clausen, "An adaptive jitter mechanism for reactive route discovery in sensor networks," *Sensors*, vol. 14, no. 8, pp. 14440–14471, Aug. 2014, doi: 10.3390/s140814440.
[42] R. Liu, Z. Weng, S. Hao, D. Chang, C. Bao, and X. Li, "Addressless: enhancing iot server security using IPv6," *IEEE Access*, vol. 8, pp. 90294–90315, 2020, doi: 10.1109/ACCESS.2020.2993700.
[43] B. Al Muhander, J. Wiese, O. Rana, and C. Perera, "Interactive privacy management: toward enhancing privacy awareness and control in the internet of things," *ACM Transactions on Internet of Things*, vol. 4, no. 3, pp. 1–34, Aug. 2023, doi: 10.1145/3600096.

BIOGRAPHIES OF AUTHORS

Ashmita Tiwari is a computer engineer at the Nepal Electricity Authority, where she plays a key role in enhancing the organization's technological infrastructure. She holds a bachelor's degree in Computer Engineering from Kathmandu Engineering College, Tribhuvan University (2022) and a master's degree in Computer System and Knowledge Engineering from Institute of Engineering (IOE), Tribhuvan University (2025). With a strong academic foundation and hands-on experience, she is dedicated to driving innovation and operational efficiency within Nepal's energy sector. Her work focuses particularly on secure, energy-constrained networks, including the IoT, Internet of Vehicles (IoV), and smart energy management systems. She can be contacted at email: 079mscsk002.ashmita@pcampus.edu.np.

Chitran Pokhrel is a computer engineer and academic researcher with a solid background in Computer Engineering with higher studies in advanced communication technologies. He has a bachelor's degree in Computer Engineering (2019) and M.Sc. in Computer System and Knowledge Engineering (2025) from Institute of Engineering (IOE), Tribhuvan University, Nepal. His research includes a wide variety of future technologies from Cyber-Physical Systems (CPS) to IoT, Next Generation Networks (SDN, 5G), and Quantum Communication Networks. He was involved in various national-level research and consultancy projects such as CPS feasibility studies for industrial automation, BTS network optimization for telecommunication authorities, and digital infrastructure design for university hospitals. He has also served as a graduate teaching assistant at the Institute of Engineering, Pulchowk Campus, where he delivered lectures and project guidance in fields of AI, network security, and programming. His research contribution includes published peer-review articles on fields of hybrid encryption for software-defined networks and transformer-based text summarization for the Nepali language. His work has also been funded by the University Grants Commission, Nepal, and the Generalitat Valenciana, Spain. He can be contacted at email: chitranpokhrel@gmail.com.

Babu R. Dawadi has completed B.Sc. Computer Engineering in 2003, M.Sc. in Information and Communication Engineering in 2008, and Ph.D. in Computer Engineering in 2021 from Institute of Engineering (IOE), Tribhuvan University Nepal. Additionally, he completed his master in publication administration degree in 2013 from Tribhuvan University. Dr. Dawadi had worked as an Asst. Director at Nepal Telecommunications Authority, an autonomous ICT regulatory body of Nepal from Dec. 2009 to Nov. 2012. Since Nov. 2012, he is a full-time faculty at the Department of Electronics and Computer Engineering, IOE, Pulchowk Campus. He deserves to teach different subjects in Computer Science and Engineering at the bachelor, master, and Ph.D. levels. Dr. Dawadi has ample experience in handling networking and internet server systems with IPv6 research networks at the Center for Information Technology (CIT), IOE Pulchowk Campus being worked as a system/network engineer and system in-charge of CIT. He worked as a consultant IT specialist at organizations like the World Bank and in different ICT policy formulations for the Nepal government. As the research operator of AI3/SOI-ASIA IPv6-only network research project, Dr. Dawadi completed his three months of research on IPv6 network from Keio University, Japan and attended several research meetings abroad as a research/training visit and conference presenter. Dr. Dawadi is awarded as a best Ph.D. fellow from Nepal Academy of Science and Technology (NAST). He runs many research projects as principal investigator under the grants provided by UGC and NAST of Nepal. He is currently serving as a post of Asst. Dean at IOE-TU, Co-chairman at the Laboratory for ICT Research and Development (LICT), and director of network, cyber security, and digital forensic wing of LICT, an ICT research lab at IOE, TU. He can be contacted at email: baburd@gmail.com.